FOR LITIGATION PURPOSES ONLY

VIA EMAIL DELIVERY

MIGUEL DEL TORAL, MARK DURNO and ENVIRONMENTAL PROTECTION AGENCY (EPA)

Re: Notice and demand for preservation of documents and electronically stored information in the care, custody, control or possession of MIGUEL DEL TORAL, MARK DURNO and ENVIRONMENTAL PROTECTION AGENCY (Hereinafter "the EPA").

To Whom It May Concern:

I have been retained by Nonresponsive in furtherance of legal action in relation to a potential conspiracy against them to defame, abuse of process, fraud and otherwise causing of tortious and constitutional harm to my clients by interfering with private litigation. The purpose of this correspondence is to demand that MIGUEL DEL TORAL, MARK DURNO and the EPA as well as their co-conspirators, agents, employees, directors, officers, attorneys and representatives - both past and present - preserve all documents, tangible things and electronically stored information ("ESI") that are in any way relevant to the $3 million lawsuit brought by MARC EDWARDS against Nonresponsive This specifically includes any communications with SCOTT SMITH and MARC EDWARDS. Electronically Stored information includes but is not limited to emails, text messages, Signal message, WhatsApps message, Twitter direct messages, Facebook direct messages, call records, and any other method of transmitting written word digitally.

It is further requested that ESI and phone records within the above scope be retained from (312)886-5253, (312) Nonresponsive (312) Nonresponsive (312) Nonresponsive and the private cell phone and all work phones of MARK DURNO including but not limited to communications by text message, Signal, and WhatsApp. Further, it is requested that records within the above scope be retained for the following email addresses: deltoral.miguel@epa.gov, Nonresponsive durno.mark@epa.gov

This notice and demand for preservation extends beyond ESI related to MARK DURNO, MIGUEL DEL TORAL, the EPA and any co-conspirator's interactions with and about Nonresponsive Nonresponsive *SCOTT SMITH and MARC EDWARDS.*

Preservation includes, but is not limited to, NOT destroying, NOT concealing, and NOT altering any paper or electronic files and other data generated by and/or stored on your computers and storage media, or any other electronic data, such as voicemail or text message.

As used in this document, "you" and "your" refers to each of the TARGETS identified in this notice including MIGUEL DEL TORAL, MARK DURNO and the EPA as well as their co-conspirators, employees, agents, directors, officers and attorneys.

You should anticipate that much of the information subject to disclosure, responsive to discovery, and/or evidence in this matter is stored on your current and former computer systems, and other media and devices, including, but not limited to personal digital assistants, voice-messaging systems, online repositories and cellphones or smartphones.

Electronically stored information ("ESI") must be afforded the broadest possible definition. It includes, by way of example and not as an exclusive list, potentially relevant electronically, magnetically or optically stored information such as:

- Digital or analog communications, both sent and received, whether internally or externally;
- Digital or analog electronic files, including "deleted" files and file fragments, stored in machine-readable format on magnetic, optical, or other storage media, including thumb drives, hard drives, floppy disks used by your computers and their backup media (e.g., other hard drives, backup tapes, floppies, Jaz cartridges, CD-ROMs) or otherwise, whether such files have been reduced to paper printouts or not;
- Word processed documents (e.g., without limitation, Word or WordPerfect documents and drafts), including drafts and revisions;
- Spreadsheets and tables (e.g., without limitation, Excel or Lotus 123 worksheets), including drafts and revisions;
- Accounting Application Data (e.g., without limitation, QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., without limitation, PDF, .tiff, .jpg, .gif images);
- Sound Recordings (e.g., without limitation, .wav and .mp3 files); Video and Animation (e.g., without limitation, .avi and .mov files);
- Databases (e.g., without limitation, Access, Oracle, SQL Server data, SAP); Contact and Relationship Management Data (e.g., without limitation, Outlook, ACT!);
- Calendar, Task Management, Diary Application Data, and personal information management (e.g., without limitation, Outlook PST, Yahoo, blog tools, Lotus Notes);
- Online Access Data, including Internet and Web-browser-generated history files, caches, temporary internet files, and "cookies" files generated on the personal and work computers of MIGUEL DEL TORAL, MARK DURNO, the EPA and their co-conspirators, employees, agents, directors, officers and attorneys.
- Data created with the use of paper and electronic mail logging and routine software;
- Presentations or slide shows (e.g., without limitation, PowerPoint, Corel Presentations);
- Network Access and Server Activity Logs; Project Management Application Data, including graphs, charts and other data;
- Computer Aided Design/Drawing Files, including drafts and revisions; and,
- Back-up Archival Files (e.g., without limitation, Zip, .GHQ).

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obliged to preserve potentially relevant evidence from both these sources of ESI, even if you do not anticipate producing such ESI.

The demand that you preserve both accessible and inaccessible ESI relevant to this matter is limited, reasonable and necessary. As you are aware, state and federal laws require that you preserve and at the appropriate time produce all sources of ESI.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Be advised that sources of ESI are altered and erased by continued use of your computers and other devices. For example, booting a drive, examining its contents or running any application may irretrievably alter the evidence it

contains and may result in the unlawful spoliation of evidence. Therefore, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve documents, tangible things, and other potentially relevant evidence.

Suspension of Routine Destruction

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI.

Guard Against Deletion

You should anticipate that your employees, agents or attorneys may seek to hide, destroy or alter ESI to prevent or guard against such actions. You should anticipate, especially where your machines have been used for Internet access or personal communications, which users may seek to delete or destroy information they regard as personal, confidential or embarrassing and, in doing so, may also delete or destroy potentially relevant ESI. Certainly, this concern is not one unique to you, your employees, or attorneys. It is simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

Preservation in Native Form

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation. You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but that may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC field.

Servers

With respect to servers like those used to manage electronic mail (e.g., without limitation, Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and email account must be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7.

Home Systems, Laptops, Online Accounts and Other ESI Venues

We expect that you will act swiftly to preserve data on office workstations and servers. You should also determine if any home or portable systems may contain potentially relevant data. To the extent that employees, agents or attorneys have sent or received potentially relevant emails or created or reviewed potentially relevant documents away from their office, you must preserve the contents of system devices, and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives or external hard drives, CD-R disks and other PDA devices, smart phones, voice mailboxes or other forms of ESI storage). Similarly, if employees, agents or attorneys used online or browser-based email accounts or services (such as Facebook, Twitter, AOL, Gmail, Yahoo Mail, or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message Folders) should be preserved.

Ancillary Preservation

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specification, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like. These documents, whether kept in paper or electronic form, must be preserved, as well as all copies of your backup tapes and the software necessary to reconstruct the data on those tapes so that there can be made a complete bit-by-bit "mirror" evidentiary image copy of the storage media of each and every personal computer (and/or workstation) and network server in your control and custody, as well as copies of all hard drives retained by you that are no longer in service.

You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and the license keys for applications required to access ESI.

You must preserve any cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. Tape drives, bar code readers, Zip drives and other legacy or proprietary devices must be preserved.

Paper Preservation of ESI in Inadequate

Hard (printed, or paper) copies do not preserve electronic searchability or metadata. They are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents and Third Parties

Your preservation obligation extends beyond ESI in your case, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, consultant, custodian, or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

System Sequestration or Forensically Sound Imaging

With respect to the parties directly managing the access and analysis of data contained in any computer system, removing their ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step. In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the model numbers of systems implicated, dictates forensically sound imaging of the systems, media and devices is expedient and cost effective.

We anticipate the need for forensic examination of one or more of these systems and the presence of relevant evidence in forensically accessible areas of the drives. Therefore, you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss. By "forensically sound" we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called "unallocated clusters," holding deleted files.

Preservation Protocols

I intend to work with you to form an agreement regarding an acceptable protocol of forensically sound preservation. If you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them.

Do Not Delay Preservation

I am available to discuss reasonable preservation steps; however, you should not defer preservation steps pending our discussions if ESI will be lost or corrupted as a consequence of delay. If the failure to preserve potentially relevant evidence results in the corruption, loss or delay in the production of evidence to which we are entitled, such failure would constitute spoliation of evidence, for which my client will not hesitate to seek sanctions and appropriate remedies including application of the adverse inference with regard to issues adversely affected by spoliation.

Attorney-Client Privilege

Nothing in this request should be construed as interfering with or impairing the attorney-client privilege of MARK DURNO, MIGUEL DEL TORAL, the EPA and their co-conspirators, employees and agents. That said, the burden in claiming that any information or communication is entitled to attorney-client privilege rests with the party asserting privilege and therefore communications, documents and data relevant to this litigation should be retained.

I look forward to receiving your call to discuss the matters raised in this notice and demand.

Respectfully,
William Moran II - Partner
Hawgood, Hawgood & Moran
(208)242-8413